APLIKASI PENGAMAN ISI LAYANAN PESAN SINGKAT PADA TELEPON SELULER BERBASIS J2ME MENGGUNAKAN ALGORITHMA SIMETRI

SKRIPSI

Oleh :

MIFTAHUL. FARID

(0734010152)

``

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS PEMBANGUNANNASIONAL "VETERAN" JATIM

SURABAYA

2011

KATA PENGANTAR

Alhamdulillaahi rabbil ‚alamin, segala puji bagi Allah Yang Maha Kuasa yang telah memberikan kekuatan-Nya sehingga penulis bisa menyelesaikan tugas akhir yang berjudul : *"Aplikasi Pengaman Isi Layanan Pesan Singkat Pada Telepon Seluler Berbasis J2ME Menggunakan Algoritma Simetri"*. Serta kepada Nabi Muhammad SAW yang telah menuntun kita semua kejalan yang lurus dan di ridhoi oleh Allah SWT.

Melalui tugas akhir ini, penulis merasa mendapat kesempatan besar untuk lebih memperdalam ilmu pengetahuan yang diperoleh selama di perkuliahan.Terutama di bidang pemrograman java. Namun demikian, penulis menyadari bahwa Tugas Akhir ini masih memiliki banyak kelemahan dan kekurangan. Oleh karena itu penulis sangat mengharapkan kritik dan sarannya untuk pengembangan ke depannya.

Secara khusus, dalam kesempatan ini pula, penulis ingin mengucapkan terima kasih dan penghargaan sebesar-besarnya kepada:

1. Kedua orang tua saya dan keluarga tercinta yang telah memberikan semangat dan do'a restunya yang tiada henti.

2. Bapak Ir. Sutiyono MT selaku Dekan Fakultas Teknologi Industri Universitas Pembangunan Nasional "Veteran" Jawa Timur.

3. Ibu Asti Dwi Irfianti,S.Kom,M.Kom, dan Ir.Kindriani Nurma W,MT selaku Dosen Pembimbing Teknik Informatika Universitas Pembangunan Nasional ”Veteran” Jawa Timur

4. Teman dekat Dan Sahabat – Sahabat yang selalu ada untuk membantu meringankan pengerjaan tugas akhir ini.

5. Semua pihak yang telah membantu yang tidak dapat saya sebutkan satu persatu.

Saya menyadari bahwa dalam penyusunan laporan ini tidak terlepas dari kekurangan dan kesalahan. Untuk itu, saya sangat terbuka bagi kritik dan saran yang bersifat membangun. Semoga laporan tugas akhir ini bermanfaat bagi saya khususnya dan bagi pembaca umumnya.

Surabaya, 11 Mei 2012

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Judul : Aplikasi Pengaman Isi Layanan Pesan Singkat Pada Telepon Seluler Berbasis J2me Menggunakan Algoritma Simetri

Dosen Pembimbing I : Asti Dwi Irfianti, S.kom, M.kom

Dosen Pembimbing II : Ir.Kindriani Nurma W, MT

Penyusun : Miftahul. Farid

ABSTRAKSI

Perkembangan teknologi telekomunikasi yang begitu pesat telah memberikan manfaat yang begitu besar. Dengan adanya teknologi telekomunikasi, jarak dan waktu bukan lagi menjadi sebuah kendala yang berarti. Salah satu hasil teknologi telekomunikasi yang sangat terkenal adalah Short Message Service (SMS). Dengan menggunakan SMS, penggunanya dapat saling bertukar pesan teks dengan pengguna lain.

Pada tugas akhir ini dikembangkan sebuah aplikasi pada telepon selular untuk memodifikasi pesan SMS menjadi cipherteks agar isi informasi dari SMS tersebut tidak diketahui oleh orang lain. Untuk pengiriman SMS sistem mengenkripsi pesan menjadi cipherteks menggunakan key yang diinputkan oleh pengirim kemudian mengirimkan ke nomor tujuan. Untuk proses penerimaan SMS, sistem akan mendekripsi masukan yang berupa cipherteks menjadi plainteks menggunakan sandi yang diinputkan oleh penerima yang kemudian menampilkan pesan asli kepada penerima. Aplikasi ini dapat dimanfaatkan oleh seseorang yang ingin mengirimkan suatu informasi rahasia kepada orang lain melalui SMS tanpa takut informasi dari pesan tersebut akan diketahui oleh orang lain.

Metode yang digunakan sistem dalam mengenkripsi dan mendekripsi pesan adalah algoritma simetri dan implementasinya menggunakan bahasa pemrograman Java 2 Micro Edition (J2ME).

Kata Kunci : Java 2 *Micro Edition*, J2ME, *Short Message Service*, SMS, enkripsi, *cipherteks, plainteks*, dekripsi, Algoritma Simetri

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi komputer dan teknologi telekomunikasi pada saat ini telah mengubah cara masyarakat dalam berkomunikasi. Dulu, komunikasi jarak jauh masih dilakukan dengan cara konvensional, yaitu dengan cara saling mengirim surat. Sekarang, dengan adanya internet, komunikasi jarak jauh bisa dilakukan dengan cara saling mengirim email atau sms (*short messaging service*). Internet juga telah membuat komunikasi semakin terbuka dan pertukaran informasi juga semakin cepat melewati batas-batas negara dan budaya. Namun tidak semua perkembangan teknologi komunikasi ini memberikan dampak yang menguntungkan bagi dunia komunikasi. Penyadapan data merupakan hal yang paling ditakuti oleh pengguna jaringan komunikasi pada saat ini.

Dengan adanya kemungkinan penyadapan data, maka aspek keamanan dalam pertukaran informasi menjadi sangat penting karena suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. Terdapat data-data yang tidak terlalu penting, sehingga apabila publik mengetahui data tersebut, pemilik data tidak terlalu dirugikan. Tetapi apabila pemilik data adalah pihak militer atau pemerintah, keamanan dalam pertukaran informasi menjadi sangat penting karena data yang mereka kirim kebanyakan adalah data-data rahasia yang tidak boleh diketahui oleh publik.

Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi merupakan kajian ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).

Algoritma kriptografi yang baik akan memerlukan waktu yang lama untuk memecahkan data yang telah disandikan. Seiring dengan perkembangan teknologi komputer maka dunia teknologi informasi membutuhkan algoritma kripografi yang lebih kuat dan aman. Saat ini, AES (*Advanced Encryption Standard*) digunakan sebagai standar algoritma kriptografi yang terbaru. AES menggantikan DES (*Data Encryption Standar*) yang pada tahun 2002 sudah berakhir masa penggunaannya. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. Dari latar belakang tersebut, maka untuk menyelesaikan penelitian tugas akhir ini, penulis mengambil topik dalam mengenkripsi teks sms menggunakan algoritma simetri AES berbasiskan J2ME.

1.2. Perumusan Masalah

Berdasarkan latar belakang masalah tersebut dapat dibuat suatu rumusan masalah, yaitu: Bagaimana cara memanfaatkan layanan SMS yang dikenal mudah dalam hal penggunaan agar dapat juga dipakai untuk mengirim

dan menerima pesan yang bersifat rahasia, dimana informasi atau isi dari pesan tersebut akan tidak mudah diketahui oleh pihak yang tidak berhak ?

1.3. Batasan Masalah

Agar pengerjaan masalah ini menjadi terarah, diberikan batasan masalah sebagai berikut :

1. Input berupa pesan teks SMS.
2. Spesifikasi SMS (panjang 1 pesan SMS) disesuaikan dengan standar teknologi *Global System for Mobile Communication* (GSM).
3. Pengujian aplikasi dilakukan pada emulator Wireless Toolkit.
4. Aplikasi ini tidak memiliki inbox sehingga pesan yang masuk tidak dapat disimpan untuk dibaca kembali.
5. Pengiriman pesan dengan menggunakan fasilitas *Wireless Messaging API* (WMA) dari *Java 2 Micro Edition* (J2ME).
6. Developer tools yang dipergunakan adalah Netbean IDE dan Netbean Platform 6.9.1 (Dual Licence : Common Development And Distribution Licence dan GNU General Public Licences Version 2 With Classpath Exception).
7. Java Developement Kit 1.6.0_21 dengan Java Hot Spot VM 17.0-b17 dan Java Platform Micro Edition Standard Development Kit 3.0

1.4. Tujuan

Tujuan dari penulisan tugas akhir ini adalah menghasilkan suatu aplikasi pada telepon selular yang dapat digunakan untuk mengirim dan

menerima pesan teks sekaligus memiliki fasilitas untuk mengamankan atau menyembunyikan informasi dari pesan yang dikirimkan.

1.5. Manfaat

1. Bagi pembaca

   Dengan menggunakan aplikasi pada tugas akhir ini seseorang dapat mengirimkan suatu informasi rahasia tanpa takut diketahui isi informasi tersebut oleh orang lain

2. Bagi Penulis

   Dengan mengembangkan aplikasi tugas akhir ini, penulis bisa lebih memahami lebih dalam bahasa pemrograman J2ME dan lebih memahami algoritma simetri.

1.6. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu :

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang, batasan masalah, tujuan dan manfaat penelitian dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini membahas dasar-dasar teori dari *Java 2 Micro Edition*, *Wireless Messaging API*, *Over The Air (OTA)* dan ilmu kriptografi

BAB III ANALISIS KEBUTUHAN DAN PERANCANGAN

Bab ini berisi tentang analisis kebutuhan pada aplikasi KriptoSMS dan perancangan perangkat lunak dengan menggunakan bahasa pemrograman Java 2 *Micro Edition.*

BAB IV IMPLEMENTASI, PENGUJIAN DAN ANALISIS HASIL

Bab ini berisi tentang implementasi dan pengujian dari perangkat lunak yang telah dibuat beserta analisis hasilnya

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dan saran yang didapatkan selama proses perancangan dari sistem serta rencana pengembangan dari perangkat lunak di masa yang akan datang.

DAFTAR PUSTAKA

Berisi tentang referensi-referensi yang telah digunakan selama pembuatan tugas akhir ini sebagai acuan yang mendukung.